

The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID MICHAEL SHACKELFORD

Appeal 2007-0715
Application 09/409,617
Technology Center 2100

Decided: May 31, 2007

Before JAMES D. THOMAS, KENNETH W. HAIRSTON, and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

THOMAS, *Administrative Patent Judge*.

DECISION ON APPEAL

This appeal involves claims 1-40. We have jurisdiction under 35 U.S.C. §§ 6(b) and 134(a).

Representative independent claim 1 is reproduced below as best representative of the disclosed and claimed invention:

1. A method for distributing computer software from a first computer system, comprising the first computer system performing:

maintaining keys of computer systems authorized to access software to be distributed;

receiving a request for software from a second computer system;

generating a message;

encrypting the generated message;

transmitting the encrypted message to the second computer system;

receiving an encrypted response from the second computer system;

determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response;

decrypting the encrypted response with the determined key if there is one determined key;

determining whether the decrypted response includes a part of the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the part of the generated message and wherein the second computer system is not authorized to access the software if there is not one maintained key for the second computer system that is capable of decrypting the encrypted response or the decrypted response does not include the part of the generated message transmitted to the second computer system; and

permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

The following references are relied on by the Examiner:

Davis	US 5,473,692	Dec. 5, 1995
Komuro ¹	US 5,991,307	Nov. 23, 1999 (filed Mar 28, 1997)
Takahashi	US 6,195,432 B1	Feb. 27, 2001 (filed Mar. 10, 1997)
Schneier	“Applied Cryptography, Second Edition”, 1996, pp. 44-46	

Claims 1, 2, 8-14, 16, 17, 21-28, and 34-40 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Davis. Claims 3-7, 15, 18-20, and 29-33 stand rejected under 35 U.S.C. § 103(a). As evidence of obviousness, the Examiner relies upon Davis alone for claims 3, 18, and 29. The Examiner combines Davis with Schneier for claims 4, 15, 19, and 30. Davis is combined with Komuro for claims 5, 6, 31, and 32. Davis is also combined with Takahashi for claims 7, 20, and 33.

Rather than repeat the positions of the Appellant’s and the Examiner, reference is made to the Brief and Reply Brief for the Appellant’s positions, and to the Answer for the Examiner’s positions.

OPINION

We reverse.

Regarding the rejection of representative claims 1 and 12, Appellant’s arguments regarding which key is used by Davis to decrypt the message having the challenge/response are persuasive. We reverse the rejection

¹ Section 8 and page 10 of the Answer inadvertently identified the Komuro reference as 5,994,307.

under 35 U.S.C. § 102(b), and since all rejections under 35 U.S.C. § 103(a) rely on Davis, those rejections are also reversed.

Appellant argued independent claims 1, 16, and 27 collectively, and since they recite substantially identical subject matter, they will be discussed together.

Regarding claim 1, attention should be drawn to the following limitations:

determining whether there is one *maintained key for the second computer system* capable of decrypting the received encrypted response;
decrypting the encrypted response *with the determined key* if there is one determined key (emphasis added).

At page 3 of the Answer, the Examiner points to col. 8, lines 54-58 of Davis as anticipating the above quoted limitations. At pages 11-12 of the Answer, the Examiner also points to col. 5 of Davis, particularly lines 47-56, as anticipating the above quoted determining step.

In col. 8, Davis discloses a similar challenge-response authentication procedure for establishing secure communications. Davis discloses exchanging public keys between two hardware agents (col. 8, lines 33-44). To provide proper context for the following discussion of Davis, it should be noted that the first and second hardware agents disclosed by Davis have been interpreted by Appellant and the Examiner as corresponding to the claimed second and first computer systems, respectively.

In col. 8 of Davis, a challenge message is sent from the second hardware agent to the first hardware agent (col. 8, lines 45-49). The first hardware agent generates a response message by encrypting the challenge

message with the *public key* (the key previously received from the second hardware agent) of the second hardware agent (col. 8, lines 49-54). The response is sent to the second hardware agent, which decrypts the response using the *private key* of the second hardware agent, which has not been exchanged and is maintained only in the second hardware agent.

It is clear that the private key of the second hardware agent is not “maintained” for the second computer system (first hardware agent), and since the private key is used to decrypt the response message, the above quoted limitation is not anticipated by Davis.

In col. 5, Davis discloses that “SK and PUK1 keys 60 and 11 are used to decrypt the encrypted original message 65 and the digital signature 80 to retrieve the transmitted message digest 75 and the original message 40, respectively.” (col. 5, lines 52-56). Also in col. 5, Davis discloses that the original message 40 is encrypted using “a symmetric secret key (“SK”) 60 via the DES algorithm to form the encrypted message 65” (col. 5, lines 33-36).

It is clear that this section of Davis does not disclose decrypting a transmitted message using an exchanged public key or a key “maintained” for a second computer system. In this section of Davis, the public key of the node initiating the communication is used only to decrypt the digital signature, which was previously encrypted using the private key of the initiating node and a message digest (col. 5, lines 40-43). The actual message is decrypted using the symmetric secret key, and it was previously encrypted using the secret key (col. 5, lines 33-35).

Furthermore, it is clear from the cited teachings at col. 5. of Davis that these techniques are not used in the challenge-response sequence used to establish secure communications in col. 8. There is no discussion of the symmetric secret key from col. 5 discussed anywhere in the description of the challenge-response sequence at col. 8. The Examiner appears to recognize this discrepancy, stating that the additional protocols disclosed in col. 5 “can be used for additional authentication” (page 12 of the Answer). While it may be true that they “can be used”, Davis chose not to do so in his disclosed method.

As mentioned above, claims 16 and 27 substantially correspond to claim 1, and the rejection of those claims is reversed for the same reasons as discussed above.

Appellant argued independent claims 12 and 25 collectively, and since they recite substantially identical subject matter, they will be discussed together.

Regarding claim 12, attention should be drawn to the following limitations, performed by “the second computer”:

providing a key to the first computer system capable of decrypting an encrypted response from the second computer system;

encrypting the response message, wherein the encrypted response message is capable of being decrypted by *the provided key* at the first computer system (emphasis added).

At pages 4-5 of the Answer, the Examiner points to col. 7, lines 44-45 as anticipating the providing step and col. 8, lines 50-54 as anticipating the encrypting step.

The disclosure in col. 7 of Davis describes a manufacturing process and discloses sending a public key to a certification system (col. 7, lines 43-46). The certification system compares the public key to previously generated keys “to ensure that each public/private key pair is unique” (col. 7, lines 46-54). The Examiner has interpreted the certification system as anticipating the claimed “first computer system” (page 4 of the Answer).

Col. 8 discusses the challenge-response sequence discussed above regarding claim 1. The cited portion states that the “first hardware system ... generates a response message by encrypting the decrypted challenge message with the public key of the second hardware agent”. However, it is clear that the “first hardware system” is not the same as the “certification system” disclosed in col. 7. The only role of the certification system is to verify that generated keys are unique during the manufacturing process. It is simply not used in the disclosed challenge-response sequence.

There is no disclosure in Davis of providing a key to a first computer system, and subsequently transmitting a response message to the first computer that is capable of being decrypted using the key that was previously provided. Instead, in Davis, the first hardware agent encrypts the message so that it may be decrypted with the private key of the second hardware agent, and not decrypted with a key the second computer system provides to the first computer system as claimed, as noted by Appellant (pages 11-12 of the Brief).

As mentioned above, claim 25 substantially corresponds to claim 12, and the rejection of those claims is reversed for the same reasons as discussed above.

Appeal 2007-0715
Application 09/409,617

In summary, we reverse the Examiner's rejection of claims 1, 2, 8-14, 16, 17, 21-28, and 34-40 under 35 U.S.C. § 102(b). Accordingly, the rejections of the remaining claims under 35 U.S.C. § 103(a) are reversed as well. Therefore, the decision of the Examiner is reversed.

REVERSED

pgc

KONRAD RAYNES & VICTOR, LLP.
ATTN: IBM37
315 SOUTH BEVERLY DRIVE, SUITE 210
BEVERLY HILLS CA 90212